IJMTST | Volume: 2 | Issue: 04 | April 2016 | ISSN: 2455-3778

Securing WSN communication using Enhanced Adaptive Acknowledgement Protocol

Mr. Sachin Acharya T

Department of CS&E, P.E.S College of Engineering, Mandya, Karnataka, India

ABSTRACT

Wireless Sensor Networking is one of the most important technologies that have different applications. The security of wireless sensor networks is a big concern. Hence for secure communication it is important to detect and prevent the attacks in network. Major focus is given on security and on detection and prevention of attacks. Adversary can create gray-hole attack and black-hole attack simultaneously. There are many methods which do not provide proper method to defend against these kinds of attacks. The Ad-hoc On Demand Distance Vector (AODV) scheme is used for detecting Gray-Hole attack and Enhanced Adaptive Acknowledgment (EAACK) mechanism is used for detecting black-hole attack in network. But only by detecting and preventing the attacks, it does not provide the better security to wireless network. Therefore, to secure network a hybrid mechanism is deployed in wireless sensor network. Security algorithm for wireless sensor networks such as CAWS and Modern Encryption Standard (MES-1) is used for secure communication. The CAWS and Modern Encryption Standard (MES-1) is an advanced cryptography method which is used for encryption and decryption process to provide special security.

KEYWORDS: *EAACK; False misbehavior reporting; Security challenges in WSN; Security attacks in WSN; MRA*

I. INTRODUCTION

Wireless sensor network is a group of specialized transducers that are deployed in particular environment to gather information. Wireless sensor network is an advanced technology with their limited energy, processing and transmission capabilities. WSN have gained popularity due to their usage in various applications in impractical environments. Wireless communication medium is inherently insecure and sensor nodes have low computational power processors, low memory, and runs on battery. In addition, sensor nodes are likely be deployed in open, physically impractical, or hostile environments where sensor nodes can be easily compromised by the attackers [1].

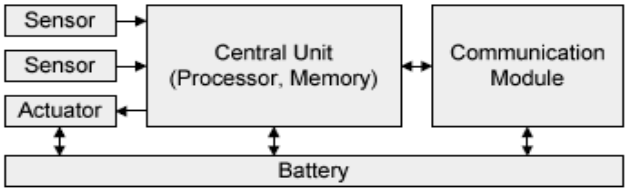

Fig 1: Structure of a typical sensor node

As shown in Fig 1, a typical sensor node consists of three subsystems. *Sensing subsystem* for data acquisition; *Processing subsystem* for processing gathered information, and *Communication subsystem* for the transmission of gathered information. Finally, the three subsystems of sensor nodes run on the energy provided by underlying battery. Though sensor nodes are deployed in impractical environments, security requirements is to be provided such as integrity, confidentiality, and availability so on.

Challenges of WSN

WSNs have many constraints compared to the traditional computer networks. This always gives significant challenges in providing security to these wireless sensor networks.
Some of them are:

A. *Wireless Medium*

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping

simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks. [2]

B. Ad-Hoc Deployment

The ad-hoc nature of sensor networks means no structure can be statically defined. The network topology is always subject to changes due to node failure, addition, or mobility. Nodes may be deployed by airdrop, so nothing is known of the topology prior to deployment. Since nodes may fail or be replaced the network must support self-configuration. Security schemes must be able to operate within this dynamic environment.

C. Hostile Environment

The next challenging factor is the hostile environment in which sensor nodes function. Motes face the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. cryptographic keys). The highly hostile environment represents a serious challenge for security researchers.

D. Resource Scarcity

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient. [3]

Security attacks and threats

Attacks on the sensor networks can be classified [4] as following ways:

- *Interruption* is a class of attack on WSN where the availability of the sensor nodes is damaged. It includes problems such as malicious content insertion, capturing the nodes, corrupting messages etc.
- *Interception* is a class of attack on WSN where the confidentiality of data that's being transmitted over the network is disclosed. It includes unauthorized access to sensor node or data within it.
- *Modification* is a class of attack on WSN where the integrity of data that's being transmitted over the network is modified. It includes the modification of the data packets or causing denial of service attack.
- *Fabrication* is a class of attack on WSN where the authentication for the transfer of control information is altered. In this sort of attacks an intruder injects false data and gains the trustworthiness.

These are all the different classes of attacks that may occur in sensor network. This classes of attacks can be rectified by using some acknowledgement schemes that ensure about the attacks on which preventive actions can be taken. But traditional acknowledgement schemes are volatile for the attacks that are explained below such as black hole and grey hole attacks.

A. *Black Hole Attack:*

A black hole attack is a kind of attack in WSN where a malicious node in the sensor network makes use of the routing information and represents itself has the shortest path to the destination node in the sensor network. After representing itself has a shortest path to destination node, the malicious node receives routing packets and does not forward packets to its neighbor nodes. This kind of malicious node is called *black hole* [5]. After the creation of this black hole in sensor network the source node sends out its data packets to the black hole believing that it's the shortest path to destination node. Thus the black hole receives all sent packets from the source node and behalf of forwarding those data packets to the destination it will simply discard those packets. So the data packets obtained by the black hole node will not arrive at the destination node.

B. *Grey Hole Attack:*

The grey hole attack was first described by Karlof and Wagner [6]. This attack is sometimes also called as selective forwarding. The grey hole attack is a kind of attack in WSN where a malicious node in the sensor network tries to stop the data packets that are passing through it in a sensor network by refusing to forward the data packets or dropping the data packets passing through them. In this

grey hole attack, the malicious node can selectively drops the data packets coming from particular sensor node. This selective dropping may create DoS attack in the sensor network. In this sort of attacks the malicious nodes may also behave like black hole and refuses to forward the data packets passing through them.

As explained above the black hole and grey hole attacks are two severe attacks on WSN with passive nature. Due to their passive nature the present acknowledgements schemes are vulnerable to this kind of attacks on WSN. The present acknowledgement schemes are explained in next section with their related work in field of WSN.

II. EXISTING SCHEMES

The nodes in WSNs assume that other nodes always cooperate with each other in data transmission. This assumption leaves the attackers to cause significant impact on the network with just one or two compromised nodes. To address this problem, IDS should be added to enhance the security level of WSNs. If WSN can detect the attackers as soon as they enter the network, we will be able to completely eliminate the potential damages caused by compromised nodes.

In this paper, we discuss some of the security schemes which are being used so far.

A. *Watchdog*

Marti *et al.* [7] proposed the Watchdog scheme. It improves the throughput of network with the presence of malicious nodes. The Watchdog scheme consists of two parts i.e. 'Watchdog' and 'Path-rater'.

Watchdog serves as an IDS for WSNs. It is responsible to detect malicious node misbehavior in the network. It detects the malicious misbehaviors by listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Path-rater cooperates with the routing protocols to avoid the reported nodes in future transmission.

The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following: 1) ambiguous collisions; 2) receiver collisions; 3) limited transmission power; 4) false misbehavior report; 5) collusion; 6) partial dropping.

B. *TWOACK*

To overcome the weaknesses of the Watchdog scheme, a new scheme named TWOACK was proposed by Liu *et al.* [8] Aiming to resolve the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination.

Upon retrieval of a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK is required to work on routing protocols such as Dynamic Source Routing (DSR) [9].

The receiver collision and limited transmission power problems posed by Watchdog are solved by this scheme. But the acknowledgment process required in every packet transmission process increased the network traffic. Due to the limited battery power nature of WSNs, such redundant transmission process can degrade the life span of the entire network.

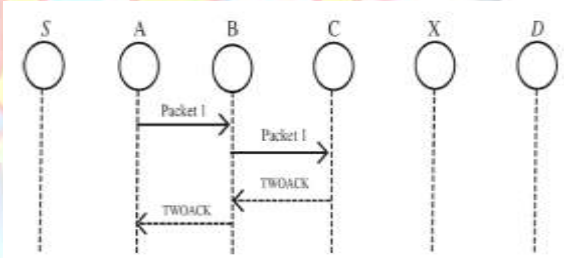

Fig 2: TWOACK Scheme

C. *AACK*

Sheltami *et al.* [10] proposed a new scheme called AACK. Similar to TWOACK, AACK is an acknowledgment-based network layer scheme which is a combination of a scheme called TWOACK and an end-to-end acknowledgment scheme called ACKnowledge (ACK). Compared to TWOACK, AACK significantly reduced network overhead while still capable of maintaining or even surpassing the same network throughput.

Within a predefined time period, if the source node S receives this ACK acknowledgment packet, then the packet transmission from source node S to destination node D is successful. Otherwise, the source node S will switch to TWOACK scheme by sending out a ACK packet. This scheme reduces the network overhead, but both TWOACK and AACK fails to detect the malicious nodes and false misbehavior reporting.

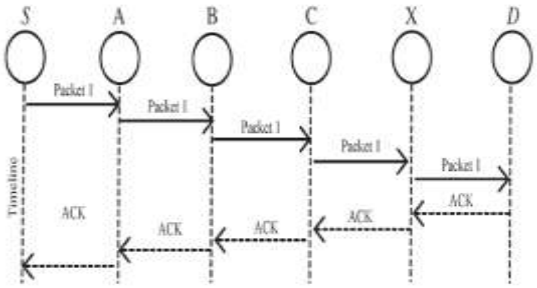

Fig 3: AACK Scheme

D. Digital Signature

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication [11]. Digital signature is a widely adopted approach to ensure the authentication, integrity, and nonrepudiation of WSNs. It can be defined as a data string, which associates a message in digital form with some originating entity. Digital signature schemes can be mainly divided into the following two categories.

1) Digital signature with appendix: The original message is required in the signature verification algorithm. Examples include a digital signature algorithm (DSA) [12].

2) Digital signature with message recovery: This type of scheme does not require any other information besides the signature itself in the verification process. Examples include RSA [11].

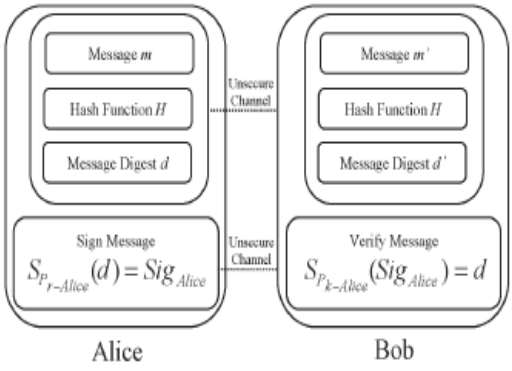

Fig 4: Communication using Digital Signature

III. ENHANCED ADAPTIVE ACKNOWLEDGEMENT SCHEME

In order to overcome the drawbacks of the above discussed scheme, the Enhanced Adaptive Acknowledgement scheme (EAACK) was introduced. EAACK is consisted of three major parts, namely, ACK, Secure ACK (S-ACK), and misbehavior report authentication (MRA)[12].

A. ACK

ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in EAACK, aiming to reduce network overhead when no network misbehavior is detected. If the ACK packet doesn't reach the source in predefined period of time then S-ACK scheme will be adopted for the network.

B. S-ACK

The S-ACK scheme is an improved version of the TWOACK. Here every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

C. MRA

The false misbehavior report can be generated by malicious attackers to falsely report innocent nodes as malicious. The Misbehavior Report Authentication scheme (MRA) is designed to detect misbehaving nodes with the presence of false misbehavior report. This scheme authenticates whether the destination node has received the reported missing packet.

To initiate the MRA mode, the node which creates the MRA packet is expected to digitally sign the packet. This digital signature can be done by only the authenticated nodes. If the digital signature does not match with the authenticated digital signature then 'false misbehavior' is reported. These nodes are labeled malicious and are neglected for further transmission.

CONCLUSION

In this paper, an enhanced and adaptive acknowledgement scheme has been proposed to introduce security into a wireless sensor network. The main advantage of this scheme is to detect false misbehavior reporting and the malicious node responsible for it. The involvement of digital signature in every MRA packet promotes authenticity and also reduces network traffic. Hence the proposed EAACK scheme helps to uphold the security goals of the wireless sensor networks.

REFERENCES

[1] Shio Kumar, M P Singh , and D K Singh,Routing Protocols In Wireless Sensor Networks- A Survey"

[2] Tahir Naeem, Kok-Keong Loo, Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009

[3] John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006 [4] Romer, K., Mattern, F. & Zurich, E.,"The Design Space of Wireless Sensor Networks,"IEEE Wireless Communication.2004

[4] M. Al-Shurman, S. M. Woo, S. Park, "*Black Hole Attack in Mobile Ad-Hoc Networks*", ACMSE'04, Huntville, AL, USA, April 2-3,2004. International Journal of Computer Science & Engineering Survey (IJCSES) Volume 1,November 2010

[5] C. Karlof, D.Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures,Special Issue on Sensor Network Applications and Protocols", vol 1 (2-3), 2003,pp.1293 –1303

[6] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5,pp. 536–550, May 2007.

[7] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1996, T-37.

[8] D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wireless networks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5,pp. 153–181.

[9] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[10] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1983.

[11] Nat. Inst. Std. Technol., Digital Signature Standard (DSS) Federal Information Processing Standards Publication, Gaithersburg, MD, 2009, Digital Signature Standard (DSS).

[12] EAACK—A Secure Intrusion-Detection System for MANETs Elhadi M. Shakshuki, *Senior Member, IEEE*, Nan Kang, and Tarek R. Sheltami, *Member, IEEE,* IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013